MARCH 1996

Information War and the Air Force: Wave of the Future? Current Fad?

Glenn Buchan

"Information War," in all of its actual and semantic variations, is a very hot topic these days. The subject has received considerable attention in a variety of forums: serious analysis for professionals, popularized accounts for lay audiences, pop futurology, and post–Cold War melodramas.[1] The national security bureaucracy is currently very active in this arena, with all of the military services and various civilian agencies and their supporting analytical organizations (including RAND[2]) establishing centers for information warfare, writing position papers, and generally grappling with the problem of how to cope with the information revolution and its consequences.

There is good news and bad news in the surge of interest in information warfare. The good news is that the public discussion could heighten the awareness of policymakers to information-related issues and possibly help focus policy-level debates. Recognizing the importance of using information effectively in war is hardly news—Sun Tzu, for example, covered the subject over 2000 years ago.[3] Moreover, there have been continuing, well-established efforts in the national security community in many critical information-related areas—electronic combat, computer and communications security, intelligence collection of all sorts, etc.—that long predate the current interest in information warfare.

Still, differences of degree can be important. Current and future changes in information technology might have the potential to alter the nature of warfare and even fundamental concepts of national security in dramatic ways. Indeed, those who posit a revolution in military affairs on the horizon cite information war as one of its key ingredients.[4] At the very least, better use of information represents one of the few remaining options for increasing the effectiveness of shrinking U.S. military forces.

The bad news is that all of the hype could impede sensible policy analysis, cloud objective resource allocation decisions, and mask real technical and operational risks and vulnerabilities. In the scramble for turf and budget shares, clear thinking about the relative value of information, in all of its various dimensions and implications for the U.S. military, has too often been a casualty. That could lead to unfortunate structural changes in organizations, inadequate analysis of critical issues, and a failure to prioritize effectively in applying information technology to warfare and broader national security concerns.

The focus of this paper is on the particular needs of the U.S. Air Force in coping with the information "revolution," although the Air Force's problems certainly cannot be divorced entirely from those of the other services or broader information-related national security concerns. Indeed, the increased emphasis on joint and multinational military operations and the use of shared information systems means that solutions to many information-related problems are going to be beyond the control of any single service. The Air Force necessarily must view information warfare from its own institutional and cultural perspective even while recognizing the broader issues involved. The objective of the paper is to help the Air Force under-

stand how to think about "information warfare" and to suggest what its priorities ought to be in coming to grips with the impact of information on its future operations. That means coming to grips with the fundamental question—How does the "information revolution" affect the conduct of military operations and, more broadly, long-term U.S. security?—is critically important to all of the military services, as well as to the broader U.S. national security establishment and those it serves.

The paper is divided into four main sections. The first addresses the problem of how to think and talk about "information warfare" and what that means for the Air Force and others. The second, and principal, section of the paper discusses how information can best be used to support combat operations and establishes a basis for setting Air Force priorities for dealing with information-related issues. The third section briefly reintroduces the broader question of the role of information in overall U.S. national security to place the traditional military issue in its proper context. Finally, there is a concluding section of summary observations.

THINKING AND TALKING ABOUT INFORMATION WAR: THE "CYBERBABBLE" PROBLEM

The ascendancy of information technology in recent years has had an unfortunate side effect: the generation of a whole new set of stultifying jargon in an area that already has a tradition of dizzying jargon and "acronymese." Part of this can be dismissed as relatively harmless word play typified by expressions such as "cyberspace," "cyberwarrior," "information highway," "infosphere," and almost any imaginable noun preceded by the adjective "virtual."[5] Arguably, there could even be some value in reminding military commanders—if they need reminding—that their concerns must extend beyond the physical boundaries of the immediate conflict (e.g., "cyberspace") and include possibilities other than physical attacks (e.g., "cyberwar"). Intellectually, the point is easy to understand, but it could raise somewhat thornier organizational issues. In particular, computer "hacking" attacks can be launched from virtually any convenient place against any other place on the earth (or perhaps above it), thereby allowing any information-intensive conflict to become as "global" as the adversaries choose to make it.

Beyond the merely annoying or the marginally useful, however, lurks a more serious concern. The danger is that the way the problem is discussed can interfere—and indeed already has interfered—with the way the substantive issues are framed and analyzed, and *that could lead to bad decisions that have unanticipated consequences.* For example, the Toffleresque view of the overwhelming importance of information in future war is appealing but needs to be subjected to rigorous critical analysis before being accepted as fact.

An important example is the expression "information warfare" itself, which is ambiguous to the point of being misleading because various organizations are defining it differently and emphasizing different aspects of the problem.[6] Although groping for an acceptable definition appears to have absorbed an inordinate amount of the defense community's attention in recent months, ambiguities still remain.[7] The basic point of contention seems to be the scope of "information warfare": whether it is basically limited to conducting or defending against "electronic attacks" on computers and related information systems or whether it also includes the whole spectrum of possibilities for using information effectively in warfare and denying enemies the same capability.

The definitional problems raise institutional issues about who does what and how the Air Force and the other services need to organize to deal with information-related issues most effectively. The narrower definitions of information warfare that essentially focus on attacking or protecting computers, databases, and the like lend themselves more readily to well-defined niches for organizations with manageable sets of tasks to perform. Unfortunately, defining information warfare that narrowly does not justify all of the attention and hype that the subject is currently receiving; neither does it solve the larger problem of where that sort of "information warfare" fits in the overall scheme of things that are of interest to the services and other defense agencies. That is particularly problematical in the emerging "gray areas" of national security that blur the distinctions between civilian police and military responsibilities, war and peace, public versus private, and economic versus military security.

On the other hand, broad interpretations of "information war" cut across the entire spectrum of military operations and involve quite disparate kinds of things (e.g., military and civilian computer security, support for targeting precision-guided weapons, defense suppression, and command-and-control attacks using a variety of means, interfering with all manner of enemy computer systems). Thus, if one were to ask who is responsible for this kind of "information warfare," the answer has to be "everybody." Ironically, that is almost certainly the right answer to the wrong question. The *right* question is the one posed at the outset: How does the "information revolution" affect the conduct of military operations and, more broadly, long-term U.S. security?

The jargon of the debate is also routinely exploited in turf and budgetary battles. This is probably one of the most familiar ways in which jargon is used and abused within and among organizations. The new jargon repre-

sents an "attention cue" that something new is afoot and that, to be among the cognoscenti, one has to be able to "talk the talk." That tends to be a precursor to laying claim to the turf (and the associated budgets). In times of shrinking defense budgets, when roles and missions of all the services and defense-related agencies are up for grabs, these kinds of turf battles can seriously affect not just the relative importance of organizations but their very survival. Adopting trendy language is a serious weapon in these wars. Potential organizational competitors may not be reassured by conciliatory language in position papers and briefings in which one group disavows any intent to dominate a hot new area. Thus, what appear to be harmless word games can mask the most serious kind of hardball. Unfortunately, such misappropriation of language does little if anything to help solve the serious problems of deciding what should be done and by whom to deal with the very real problems of protecting U.S. security in an information-rich world.

Even more fundamentally, focusing on "information warfare," however defined, leads to a confusion of means and ends that tends to stand basic strategic thinking—the definition of overall objectives followed by the evaluation of various alternative means to accomplish those objectives—on its head. This is another area in which reassuring words on viewgraphs are not likely to be sufficient to overcome the institutional pressures. That, in turn, leads to a focus on inappropriate, intermediate measures of effectiveness for the "information war" at the risk of losing sight of the linkage to more fundamental goals. To recognize the danger, one need only remember how distorted a picture "body counts" presented as military measures of effectiveness and various social indicators presented as measures of the success of the pacification program provided of progress in the Vietnam War. Although "bit counts" or something equally crude will hopefully never become the body counts of the 1990s, war games revolving around information continue to provide anecdotal examples of analysts and planners using inappropriate measure of effectiveness to prove they were winning the "information war" with little reference to the ends that information is intended to serve in combat.

An example of this particular phenomenon at work is the expression "information dominance," which is frequently cited as a goal of information warfare. Now, the notion that one should know as much as possible about one's enemies as well as one's own forces while trying to keep the enemy as much in the dark as possible is hardly going to come as a surprise to any student of military affairs. Indeed, Sun Tzu emphasized the relative importance of what amounts to "information dominance" without burdening readers with the jargon. If that is all information dominance means, then it amounts to a tautology that adds nothing of substance to contemporary discussions of military strategy and operations. On the other hand, including "information dominance" in the list of "core competencies" of the Air Force is largely benign, even helpful to the degree that it elevates the relative importance of developing and maintaining information-related expertise in the Air Force of the future.

As an operational objective, however, information dominance is likely to be hard to define or measure, particularly in the complex military-political situations that seem to typify the post–Cold War era, and could well be very difficult to achieve in any meaningful way in many classes of conflicts. For example, how does one define, measure, and achieve "information dominance" in a Somalia-like conflict, in which the opposing sides have such disparate characteristics and operational objectives? How do U.S. forces using high-tech sensors, communications, and information systems achieve "information dominance" in a very complex political-military campaign against an indigenous, entrenched opposition that can meet most of its military needs with simple means (e.g., "move to smoke" as a general rule of engagement, drums, word of mouth through human networks) or carefully selected application of high technology (e.g., fiber-optic cables) and when both sides are subject to scrutiny by worldwide news organizations (e.g., Cable News Network)? Is it even a meaningful question? Pursuing "information dominance" as a specific operational objective provides both military commanders and analysts with incentives to focus on the wrong part of the problem (e.g., the body-count mentality) and confuse overall means and ends, a problem that would almost certainly be reinforced by any institutional structure that includes organizations with explicit responsibility for information warfare, since those organizations will be obliged to establish objectives and demonstrate that they are meeting them regardless of how they relate to the larger military campaign objectives.

Instead of dwelling on "information dominance," a back-to-basics approach that relates specific information-related tasks to broad operational objectives appears more useful. Specifically, U.S. military commanders ought to be asking the following questions in any particular situation:

- What information does the United States need to conduct any particular operation, and how can that information be obtained?
- Can the United States conduct information-intensive operations in a hostile environment against a competent adversary?
- Can the United States deny the enemy the information necessary to conduct effective operations to meet *its* objectives and to thwart U.S. operations? How?

Not only will that sort of approach lead to more direct answers to meaningful operational questions, but it will also tend to *disaggregate* disparate elements that are sometimes lumped together as "information warfare" (e.g., computer security, high-tech psychological operations, adaptive mission planning, precision strike) into more logically coherent pieces that can then be integrated with other combat tasks into effective operational plans.[8] That, in turn, should lead to more precision in planning.

CONDUCTING AIR FORCE OPERATIONS IN THE INFORMATION AGE

The Air Force's *raison d'être* has long been gaining control of the air, destroying critical targets on the ground, moving personnel and materiel around the world by air, and providing various kinds of critical support from space. All of these operations could benefit substantially from improved use of information. Moreover, Air Force systems are likely to play an important role in collecting, processing, and distributing much of that information.

In the complex post–Cold War world, U.S. military forces could be called upon to perform a very broad spectrum of operations almost anywhere in the world, frequently using very advanced systems, sometimes with very little advance warning. Even with better technology, this is going to be very challenging. In fact, *orchestrating the process of getting the right information, putting it into a usable form, and getting it where it needs to go in a timely manner is one of the most important problems that the Air Force has to solve.*

Using Information Effectively

Taking maximum advantage of the new information technologies will affect everything the Air Force does from the way it designs and procures weapon systems through the way it supports and plans missions to the way it conducts and manages operations. RAND's ongoing analysis on many of these topics suggests that the Air Force needs to do considerable work to allow its forces to function as effectively as possible *even in a relatively benign environment.* The Air Force is aware of many of these problems and is working actively to solve them. *Dealing with this broad spectrum of "information operations" should be the Air Force's first priority in taking advantage of the information revolution to support its combat operations.* That is the basis for making everything else work.

If the information revolution really is to have the impact on military affairs that its most ardent proponents suggest, fundamental changes will have to occur in the way the United States designs and acquires new systems. In particular, as the stealth experience suggested, avionics and electronic systems designers are going to have to have a place at the table during the preliminary design phase of new systems to make sure designs accurately reflect the relative importance of information systems on the overall effectiveness of the system. Similarly, system design and acquisition procedures will need to be changed to allow almost continuous modifications and upgrades to computer hardware and software, as well as periodic changes to communications and sensor systems, with a minimum of bother and expense. RAND's analysis of the B-2 bomber, for example, showed that information system modifications were among the most important improvements that needed to be made to the bombers to make them effective and that making those modifications is much more difficult because of the way the aircraft was designed and procured.[9] The Secretary of Defense's initiative to create Integrated Product Teams to develop future systems is intended to help alleviate some of these problems.

How far to go with these sorts of changes depends fundamentally on the validity of the Toffleresque hypotheses about the relative importance of information in future warfare and the promise of information technology. While intuitively appealing, and almost certainly valid to a point, the *broader hypotheses remain to be fully tested analytically and empirically.* This is an important area for continuing research.

At least as fundamental as the problems of building the right systems and keeping them up to date are the difficulties of providing the sort of information those systems need to be used effectively. For example, the defense community failed to prepare adequately to support the newest generation of precision-guided weapons and stealthy aircraft. They need information beyond what is available in the standard set of intelligence products and services; they need it more quickly; and appropriate planning systems have not been widely available.[10] Key problems included security restrictions on new weapon programs that complicate involving the intelligence community early in a program, lack of operator involvement, and the relatively limited resources available in the intelligence and support communities (e.g., the Defense Mapping Agency) to solving these problems.

Some of the problems are technical, but the more intractable problems are institutional. The Air Force has recently recognized the organizational problem of getting weapon developers, operators, and the intelligence community to talk to each other and has implemented a formal process to try to solve it. The Air Force has created a new acquisition document known as the intelligence support plan (ISP),[11] which will define the intelligence infrastructure required to support a specific weapon system. The Office of the Secretary of Defense (OSD) is examining the Air Force ISP process, as well as the Army and Navy approaches to providing intelligence support for guided weapons, and will select a preferred approach as a tem-

plate for future weapon system acquisition programs. The adequacy and resilience of this approach to integrating the information-related activities of disparate organizations remains to be fully demonstrated, but at least it is a start.

Institutional problems extend to career paths within the military, as well as to basic organizational structure. Intelligence seems to be falling even farther behind some of the other Air Force career specialties, for example,[12] and some of the traditional approaches to improving the lot of intelligence officers are likely to do more harm than good to the overall process of using information effectively to support military operations. Moreover, the problem extends beyond the narrow world of intelligence to the broader question of information in general and is at the heart of some of the fundamental questions about how "information warfare" is viewed by the national security community.

There is a twofold problem: determining how to increase the relative importance of information and information-related specialties in the overall scheme of things and how to integrate information effectively into military operations. The usual approach to upgrading career specialties in the military involves creating separate commands and organizations (e.g., "centers"). Unfortunately, there is a natural tension between this approach and the need to integrate information more effectively into the entire spectrum of operations. Creating separate organizations tends to isolate rather than integrate, confuse means and ends, and mix disparate functions in an inappropriate manner. The problems that the Air Force has traditionally had in effectively integrating space into Air Force operations are a case in point. That is precisely the danger of the current institutional reactions to the discussions about "information warfare." While institutional reactions increase the visibility of information to the U.S. military, creating centers of information warfare and similar information-focused organizations is likely to be counterproductive. *Instead, what the Air Force and the rest of the U.S. military need to do is focus on integrating information considerations effectively into all of their operations and organizations.* How best to do that while upgrading information-related career paths within the service remains an issue. Defining "information dominance" as an Air Force "core competence" might help elevate the importance of information specialists in the Air Force hierarchy, but creating a suitable organizational structure in which these specialists can be effective is a more fundamental and difficult problem.

So far, all of the problems we have discussed affect only the preparation for combat—designing and building systems, collecting and analyzing intelligence, mission planning, etc. Solving these peacetime problems is still only an "admission price" into the game. There are more problems to solve if the "information revolution" is really going to have a dramatic impact on combat itself. One of the most fundamental hypotheses about the potential of the information revolution is that it could allow battle managers to monitor virtually everything of interest on a battlefield nearly continuously and to adjust operational plans accordingly in near-real time. That would represent a revolutionary change in how the military does business. Whether it is actually feasible and, if so, whether it is worth the trouble and expense of doing remain among the most profound (and unresolved) issues associated with warfare in the information age. Indeed, the real question is how far it is worth going down this path, considering technical feasibility, operational payoff, and cost. Then, the challenge is in deciding how to make it happen. Specific issues include the following:

- What are the payoffs for various levels of adaptive planning in combat operations?
- How much planning flexibility is technically feasible and affordable?
- Does the Air Force retain current planning vehicles, such as the Air Tasking Order (ATO)? If so, how will it change? If not, what will replace it?
- How does the military adjudicate the problem of information flow versus chain of command? How does it reconcile "commanders' prerogatives" with combat efficiency while avoiding chaos?
- How far can combinations of various types of sensors on different platforms go in providing a complete, operationally useful, and continuous picture of the battlefield? What is the most cost-effective combination of sensors, platforms, and processing facilities to provide the necessary information?
- How can the damage assessment problem be solved adequately, particularly when more-sophisticated weapons that rely on relatively subtle damage mechanisms are used?
- How does the United States construct a command, control, communications, computers, and intelligence (C^4I) architecture to wire all of this together, satisfying the needs of all the disparate users?
- What are the impediments to introducing improved technology effectively? (In a recent major joint operational exercise, TANDEM THRUST, which was designed to exercise new planning systems and procedures, RAND analysts witnessed planners still relying on grease pencils and manual planning in spite of the new systems.)

All of these issues are being investigated intensively by RAND and others, and while progress has been made

in some areas, the fundamental questions remain unresolved.

Coping with a Hostile Environment

All of these problems would be hard enough to solve in a benign environment. Making it all work in combat against competent enemies complicates matters considerably. Second in priority only to meeting the Air Force's basic information needs should be a concern about how vulnerable its information systems are, how serious the potential threats are, and what can be done to reduce critical vulnerabilities.

First, the United States is likely to be more critically dependent on information-related systems and strategies and more vulnerable to their disruption than most potential adversaries. Vulnerability is the "flip side" of the leverage that information offers. Moreover, since most future military campaigns that the United States might fight are likely to be a long way from home, potential vulnerabilities could be global—collection and processing centers at either end, communications between the U.S. homeland and the theater of combat, etc. Evaluating the relative importance of the whole spectrum of vulnerabilities should have direct bearing on fundamental C^4I architectural and operational decisions about how to structure military information systems (e.g., where and how to process and analyze data, how much to centralize, how much to rely on high–data-rate communications). Thus, in addition to all the standard concerns about jamming communications systems, countermeasures against surveillance systems, and the like, the United States will have to be particularly concerned about the capabilities of an enemy to disrupt, destroy, distort, or otherwise interfere with its ability to use information effectively. All manner of potential threats are possible, including standard attacks on critical facilities, such as planning centers (e.g., the "Black Hole" in Riyadh where the daily air campaign planning for the Gulf War took place), commando attacks even against facilities in the United States, or electronic attacks of various sorts. That raises concerns about both physical and electronic security, as well as the degree of centralization of facilities, databases, and information that is prudent.

The question of centralization—and the resulting trade-offs between efficiency and vulnerability—is a classical one, but information technology and institutional complications regarding responsibilities add some new wrinkles. Where issues of centralization are concerned, organizations, databases, and hardware systems need to be viewed differently. For example, common—or at least compatible—hardware and software are going to be virtually obligatory for many military applications. However, common databases may or may not be achievable or even desirable depending on the particular application. For example, different users will need different sorts of information and may not, therefore, need to tap a common database. Reducing the centralization of databases should also reduce their overall vulnerability to disruption, destruction, corruption, or other forms of compromise. How practical decentralization of databases is, however, in view of the need to share common data to achieve full operational integration, remains a fundamental operational issue.

Computer vulnerability has long been recognized as a part of the overall problem of vulnerability of information. In fact, it is currently receiving particular attention from the Air Force, which apparently sees this as the defensive side of "information warfare" and attaches particular importance to it.[13] The Air Intelligence Agency routinely investigates incidents of computer "break ins" at Air Force facilities and sends teams out regularly to help with computer security. Both the Air Force and the Department of Defense (DoD) routinely test their systems to see how successful "hackers" are likely to be at breaking in undetected. In a recent series of exercises, for example, the Defense Information Systems Agency (DISA) reported that, in mock attacks on more than 8,000 unclassified DoD computers, it successfully broke into more than 88 percent. Only 5 percent detected the break-in attempt, and only 5 percent of those reported it.[14] In similar experiments conducted internally, the Air Force has done slightly better. In fact, in a recent DISA experiment, the Air Force reportedly did much better than the other services. Still, in the absence of safeguards, breaking into unclassified computers hooked into the Internet appears easy for skilled hackers. That is likely to be of even more concern in the future as budgetary pressures force the Air Force to rely more and more on commercial systems for processing and transmitting information. The defensive aspects of this issue are under active study at RAND and elsewhere.[15] Although steps—often straightforward ones—to mitigate some risks can be identified, the unfortunate fact is that such steps are frequently not taken or not repeated when system configurations change.

The Air Force C^4 Agency is currently instituting safeguards for the Air Force's unclassified computers and appears to be confident that they will be adequate.[16] It also seems relatively sanguine about the security of classified computers, at least against tampering by outsiders. Similarly, it seems confident that current antivirus protection is adequate. Whether that safety extends to other kinds of electronic threats, such as Trojan horses, "logic bombs," and nefarious "surprises" planted in computer hardware, is not clear. In fact, it is unclear how confident the Air Force *should* be that it can protect its computers and databases from electronic attack and, considering the

spectrum of potential enemies, how serious the problem really is. That remains an analytical issue and is part of the broader question of how well an Air Force that runs on information can protect itself against a broad spectrum of threats.

Because the Air Force will increasingly depend on information systems devised by others—the other services, other defense-related agencies, and the private sector—its information-security problems will become more complex because guaranteeing the security of these systems is beyond the Air Force's control. Dealing with these issues will require a more integrated approach than the U.S. national security community has displayed so far.

Denying Enemies Effective Use of Information

Trying to deny enemies the ability to use information effectively has always been an important part of warfare and is an integral part of normal combat operations. However, the heightened awareness of information-related issues and interest in exploiting potential vulnerabilities in others have focused interest on this broad class of activities, which might be considered the offensive side of "information warfare." (Again, referring to it this way has logical problems, particularly in terms of organizing to do it, but by whatever name it is called, the subject itself merits attention.) There are three main classes of issues:

- How important is this particular class of operations?
- How can they best be accomplished, and where do all of the "new tricks" (e.g., computer viruses, manipulated data, "nonlethal" weapons) fit in?
- What are the organizational implications?

Predictably, the answer to the first question is, "It depends." There is a danger that the trendiness of attacking information systems will cause people to lose sight of the fact that such operations, like any others, must serve particular military and political objectives and may have to compete with other missions for priority and resources. The difficulties with predicting the effects of such attacks have always been an issue, and the traditional intelligence problems of identifying suitable vulnerabilities and determining the best ways to execute such attacks are likely to become even more formidable in the future. Also, Sun Tzu notwithstanding, denying an enemy the use of information is not always a particularly wise idea. An obvious example from the "old" nuclear days was the theology of limited nuclear attacks in which an attacker would probably choose to leave warning systems intact to help convince the victim that an attack was really limited and might also leave the enemy's control system intact in hope of providing the victim with both an incentive and the means to keep a conflict under control. Probably an ideal objective would be to *control* the information adversaries have and which of their information-related systems continue to function. In fact, deception as a tactic is likely to become even more widespread in the future because of the broad availability of suitable low-cost technology with "global reach."

How well such a strategy is likely to work, how important it is, and how to do it remain issues, and none can really be addressed satisfactorily in the abstract. Still, general observations may open the way for more detailed analysis in specific cases. To begin with, the United States is likely to face a very wide range of situations and potential opponents, and the relative importance and likely effectiveness of "information attacks" (whatever that turns out to mean) are likely to vary enormously. First, there are relatively few, if any, potential adversaries whose military capabilities and societal well-being rely as heavily on high-tech information systems as the United States does. Thus, there may be no "mirror images" to attack. Even if there were, those societies might also become the most adept at protecting their information systems, and who eventually wins that game of move and countermove is unclear at present.

Opponents at the other end of the spectrum may be both more common and harder to deal with. For example, in the Somalia intervention, the local warlords had their own means of getting information, communicating, and controlling their forces that were largely immune to any counters that the United States might be able to mount. Thus, they had no particular difficulty acquiring and managing the information that they needed to solve their specific problems.

The ready availability of information in the future to those with even rudimentary technical capability represents yet a different side of the problem. The increasing availability of high-quality commercial communications, navigation, and surveillance information to virtually anyone who needs it—plus access to the Internet and other worldwide computer networks—may be a great equalizer in future "information wars." Almost anyone will be able to play, and denying access to "bad actors" may be difficult or impossible technically, politically, or legally. If that comes to pass, the United States may never again be able to surprise an opponent with a massive undetected maneuver, as Schwarzkopf did in the Gulf War with his famous "left hook" flanking attack on the Iraqi forces in Kuwait. Of course, it may still be possible to manipulate such information, even if it comes through commercial systems, but that will be a delicate proposition, and its feasibility and wisdom will require careful examination.

The classes of opponents that might prove most vulnerable to information-related attacks may be those that

are relative neophytes in modern warfare that are just making the transition to high-tech warfare (e.g., integrated air defense systems) and are dependent on new systems but not necessarily comfortable enough with them to be able to protect themselves from electronic or physical attack. Prewar Iraq is typical of that sort of state. There also may be non-nation–state actors (e.g., criminal syndicates, terrorist groups) that are more vulnerable to electronic attacks (e.g., "zeroing" bank accounts, to take a topical example) than physical attacks.

Doing a broad assessment to categorize potential opponents by their potential vulnerability to "information attacks" should be one of the prerequisites for determining how much effort the United States should put into developing this kind of capability. For example, the "information attacks" could extend beyond attacks against traditional military targets, just as more-traditional methods frequently do. Attacks on the information infrastructure of warring nations could play an increasingly crucial role in future warfare. Such attacks will, of course, be most damaging to nations that rely heavily upon their information infrastructure. (That being the case, there is probably no finer target for such attacks than the United States, with the other First World nations following. Clearly, a future enemy would enjoy a "target-rich" environment in attempting information operations against the United States.) What is not clear is the scale on which the United States would be able to conduct information operations against a Third World enemy and what effects such attacks are likely to have.

Information infrastructure attacks may be conducted by special operations forces operating from enemy information hubs (e.g., a telephone central office, microwave relay tower) or even by "computer nerds" sitting at terminals on the other side of the world. Attacks need not focus on the destruction of these assets when simply coopting them and turning them to the ends desired could be sufficient. Direct-action missions targeted at information choke points, perhaps broadcasting an "all clear" signal moments before an attack, may well be a type of information warfare that could make a real difference in the tide of battle and cause rapid capitulation.[17]

In establishing an overall strategy for "information attacks" of all sorts there are still fundamental analytical questions to resolve. They include the following:

- How hard should we try (i.e., what is the relative value of these kinds of attacks as opposed to other kinds of operations)?
- How will the attacker tell if the attack has worked, and how confident should he be (e.g., could one be confident enough, for example, that an air defense network had been rendered ineffective by an attack on the air defense command and control network that the pilot would be willing to fly through it without attacking specific surface-to-air missile sites)?
- What are the best ways to do such "information attacks"?

Traditional weapons may be suitable, perhaps even preferable, for many kinds of attacks against opponents' information systems. However, one of the things that has captured the imagination of both experts and laymen is the possibility of relying more heavily on different approaches—e.g., computer viruses and the like, manipulation of data, "nonlethal" weapons that work directly against electronic systems. Some of these techniques may very well be appropriate. Indeed, while some are quite new and largely unproven, others are quite mature and well-understood, at least among the cognoscenti. Some of the techniques may offer better ways to solve formerly intractable problems. For example, one of the difficulties with traditional approaches to command and control attacks has always been that destroying nodes might well be ineffective because there were so many and because the attacker did not understand the enemy C^3 system well enough to construct an effective attack. By contrast, it is at least conceivable that a well-designed electronic attack could disrupt an entire *network* rather than selected nodes alone. If that were to work, it could offer a new kind of capability.

These techniques have potential problems, however. Many are likely to work only once and then for only a short time. Existing vulnerabilities tend to be fragile and easily repaired once identified. Moreover, information infrastructures tend to grow and mutate. Weaknesses that existed last week may be corrected with a new software release. On the other hand, experience suggests that some vulnerabilities tend to reappear because of a lack of configuration control in both public and private computer networks, which may make it possible to exploit weaknesses that users think they have eliminated.[18] Network routing tables can change, redirecting critical information from one path to another. In such a dynamic environment, it may be difficult or impossible to carefully plan and execute information operations in a reliable fashion. Further, a clever enemy may leave "bait" lying unprotected to entice operatives to react in a predictable fashion. For these reasons, a precision strike against information resources is less likely to succeed, particularly against an enemy that has both technological sophistication and vigilance.

The fragility of these techniques leads to another problem: extreme secrecy. While guarding the techniques may be necessary to a point, holding them too closely raises two kinds of potential problems. First, if plans for attacking enemy information systems, for exam-

ple, are too tightly held, they might well conflict with another part of an overall campaign plan that might actually use some of those systems. At the very least, something might get "overkilled." Second, there may well be a conflict of interest at the national level between developing offensive techniques that could be used against an enemy that used American equipment, for example, while holding that knowledge very tightly to preserve the option, and withholding the knowledge from the "defensive" side of the house that is trying to protect the United States from "information attacks."

Finally, some of the fascination with the "nonlethal" nature of some of the new approaches may be misplaced. In the first place, some are not all that "nonlethal." For example, microwave weapons that blind people while destroying electronic systems or electromagnetic pulse (EMP) weapons that cripple aircraft flight-control systems causing planes to crash are hardly benign. Nor are implanted flaws in computer chips that cause military (or civilian) vehicles' brakes, steering, or safety-related systems to fail. Indeed, these could be considered terror weapons.

The point is not that minimizing physical damage has no value—it well might in some circumstances—or that disabling something electronically might not be more humane than blowing it up—depending on the circumstances, it could be. Rather, it is important not to get carried away with the illusion of antiseptic war. As a former commander in chief of the Strategic Air Command once put it after hearing a series of briefings about the (nonviolent) wonders of strategic airlift and airborne refueling, "Sooner or later, someone has to kill somebody!"

He was right. In fact, preliminary research at RAND suggests that some of the most effective uses of "information attacks" may be in conjunction with more traditional methods of attacking targets. Thus, they might make killing more efficient. While it is conceivable that a clever attacker could, under certain conditions, manipulate an enemy's information thoroughly enough to induce a premature surrender or in some other bizarre fashion produce a "bloodless" victory, those cases have to be the exception rather than the rule. War is still about violence, and the illusion that new weapons can take the horror out of war is a disservice to rational policymaking. Instead, all of the new weapons need to be evaluated the same way as the old ones: What do they do, how well do they do it, how much do they cost, and under what conditions might they be useful (which certainly allows considerations of such issues as collateral damage)? Basically, they are simply additions to our bag of tricks that may offer attractive options in appropriate situations. Defining "attractive" and "appropriate" remains an analytical issue.

The Organizational Dimension

That leaves the organizational issue: Who does what in this arena? The general answer should be that, to be fully effective, appropriate offensive information warfare "weapons," for example, should be added to the repertoires of all elements of forces concerned with the whole spectrum of offensive application of force, from psychological operations to tactical deception to the whole range of ground-attack operations. Not only would such integration make using the weapons effectively much more likely, but also it would help place "information warfare" techniques and technologies in a more useful operational context. Similarly, the defensive side of information warfare needs to be infused into all the organizations responsible for developing, procuring, and operating information systems. Better exploitation of information remains literally everyone's business. Integrating information-related concerns into the whole spectrum of military operations would, over time, help guide decisions about the relative weight to give "information warfare," as opposed to more traditional approaches. That, in turn, *could provide a basis for the Air Force* (and perhaps other services) *to evolve into a totally different kind of organization with a different culture and substantive emphasis.* The evolution would be almost Darwinian: It would happen if and when substantive conditions warranted. In the meantime, the Air Force needs to establish information-related career paths within its existing structure and avoid creating a "geek command" that would isolate rather than integrate officers with expertise on information technology and applications.

This sort of organizational approach should also produce a more specialized, differentiated set of skills and responsibilities than lumping quite disparate specialties together into an umbrella "information warfare" organization. It would also help resolve the inevitable "roles and missions" conflicts that will arise among competing services and agencies. That is likely to be particularly important in the relatively short term when critical information-related skills are likely to be in too short supply to permit much duplication in functions among organizations. For example, some of the critical skills are more likely to exist in such organizations as the National Security Agency (NSA) and the Central Intelligence Agency than in the uniformed services. Sorting all this out should be part of the national-level debate on roles and missions of the military, the intelligence community, and the rest of the defense community.

So far, the Air Force has rejected the concept of an information-warfare command or anything equivalent. That is good. Establishing such a command would retard rather than promote the necessary integration of information-related considerations into the whole spec-

trum of Air Force operations. Also, the Air Force has given XO (Plans and Operations) on the Air Staff and Air Combat Command (ACC) among the major commands primary responsibility for information warfare. That is also good: Operations should "drive the train."

However, the organizational issues are far from resolved. The responsibilities and rules of the newly created (or, in some cases, renamed) organizations, such as the Information Warfare Center and the Information Warfare Squadron at 9th Air Force Headquarters, as well as the more established organizations, such as the Air Force C4 Agency, remain to be sorted out.[19] Similarly, creating information-warfare organizations within established groups could be counterproductive if the net effect is to isolate rather than integrate the responsibility for information warfare–related considerations. At best, the jury is still out on how well these institutional solutions are going to work. Ironically, the existing institutional structure was probably adequate if it had been used effectively.

"We Will Serve No Revolution Before Its Time"

The hype about the "revolution" in information technology and its potential impact on warfare and the debate about whether the overall effect is revolutionary or evolutionary may be interfering with sensible discussion of what the changes really mean. First, in one sense, it is not particularly important whether the changes are "revolutionary" or not: Good ideas should be of interest however they are labeled. Second, there are several different things going on, all of which involve the temporal dimension of technical change and its military impact. In particular, a list of potential pitfalls that can occur in introducing new technology might include the following:

- *The technology is too immature.* It either does not work well enough or can be countered relatively easily and cheaply.
- *The technology is too expensive.* This has been a perennial problem with "smart" weapons, for example. It has taken decades to develop relatively cheap smart weapons, and the battle is still not completely won (e.g., developing cheap, effective precision-guided submunitions remains a technical challenge). In particular, the "buy-in" costs for new technology can be a problem early on.
- *The technology may be applied improperly.* Organizations may not adapt rapidly enough to new technology either operationally or strategically. Alternatively, they may simply try to apply it to the wrong problem.
- *It may not be possible to introduce new technology rapidly enough or on a large enough scale to be decisive if time is relatively short.* This is simply a problem of scale and time.

Not all of the information-related technologies are developing at the same rate, and lumping them together even conceptually is likely to be a mistake. For example, precision-guided munitions and advanced sensors to monitor battlefield operations, which are key elements of the postulated revolution in military affairs, have been evolving for decades.[20] Laser-guided bombs were among the first precision-guided weapons to be employed in combat several decades ago in the war in Vietnam. However, the "revolution" associated with large-scale precision strike has been a long time coming and is only now on the horizon. Expanding the concept of precision strike from isolated attacks on small numbers of individual targets to a broad operational concept of large-scale precision attack requires maturation of a number of different technologies, and that has taken a considerable number of years. Thus, even when a new technology "works," as precision-guided weapons have, a lengthy gestation period can be required for a "revolutionary" change in warfare to occur.

In other cases, new technology was too immature to be really effective even when it was introduced into combat. For example, the remotely implanted ground-based sensors designed to monitor infiltration along the Ho Chi Minh Trail were probably a good idea in principle, but were ineffective because the technology of the period was simply not up to the task (e.g., among other things, the sensors were too easily spoofed). With 1990s technology, such a sensor network might be extremely effective. The wartime application in the 1960s was simply premature.

Cost is always an issue and is even more important in times of fiscal austerity. There has always been a natural tension between the promise of a new technology and the opportunity costs that the initial R&D investment typically entails. The dramatic cost reductions in information-related technologies in recent years are one of the most attractive features of the "information revolution." Still, rigorous analysis is necessary to define the best course for the Air Force to take to exploit the potential opportunities effectively.

Even the best technology cannot be decisive militarily if it is used improperly or applied to largely irrelevant problems. For example, when laser-guided bombs were introduced in the Vietnam war, they certainly increased the effectiveness of U.S. bombing against point targets. However, that had very little effect on the overall progress of the war, mainly because technology was being asked to solve the wrong problem. It just solved the wrong problem more efficiently.

Problems of scale and time are intertwined with investment decisions and overall strategy. The much-analyzed cases of the German "wonder weapons"—the V-1, the V-2, and jet aircraft—illustrate the familiar problem of potentially effective weapons introduced too late and on too small a scale to have much effect on an ongoing conflict, unlike, for example, the Allied development of radar during the war. The United States has had a scale problem with its development and deployment of conventional cruise missiles, in spite of their successful use in the Gulf War and more recently in Bosnia. Deploying them and being able to support them in large enough numbers to be decisive in a major conflict remain problems even now. Fortunately, unlike the Germans in World War II, the United States so far has had the luxury of pursuing these programs during a time of relative peace. Still, a major change in the way the United States fights wars could take some time to implement, even in an era of dynamic technological change.

All of this suggests that timing is quite critical in introducing and exploiting new technology and that a side that moves too early can miss the mark. Interestingly, that is not necessarily "counter-revolutionary." Indeed, Andrew Marshall, the "father" of the current notion about a potential revolution in military affairs, likes to use the example of the German *blitzkrieg* to demonstrate that a military revolution can occur when one side effectively exploits relatively mature technology by developing new operational concepts. In fact, a mature-technology warmaker might be able to crush "new entries" and really dominate them because of its greater experience with the technology than its potential competitors.

On the other hand, because of the broad range of information-related technologies, *no single paradigm is likely to be adequate* to predict their evolution and potential impact. For example, the nature of some kinds of information technology may permit new users to "skip a couple of grades" and become "peer competitors" in specific niches early on. That could allow the "weak" to challenge the "strong" and is, of course, at the heart of much of the concern about U.S. vulnerability to "information warfare."

Unfortunately, assessing these possibilities analytically is quite challenging. In general, the tools currently available are not up to the task of answering even the "simple" questions about the national security implications of the information revolution. This is an area that begs for more research.

NEW DIMENSIONS OF SECURITY: INFORMATION AND THE BROADER ASPECTS OF NATIONAL SECURITY

Dealing with the military side of "information warfare" begs the more fundamental question of how to protect American society in general from attacks on its information infrastructure. The Air Force needs to understand the broader problem in formulating its own approach to information warfare. There are three basic questions:

- How serious is the problem?
- What can be done, and how well is it likely to work?
- Who should—and who *can*—do it?

This problem has certainly captured the imagination of authors and raises some intriguing questions about the very nature of conflict. For example, as Jack Ryan, Tom Clancy's fictional hero, observed, it could be a little difficult to tell in the information age if a nation were at war and, if so, with whom. In addition to potentially hostile nations, plausible bad actors could include criminals, hackers, terrorists, insurgents, and industrial interests. A particularly attractive feature of this kind of "warfare" is that, while it requires considerable expertise, it probably does not take much in the way of resources or involve much physical risk to the attackers. Thus, it may offer many would-be Davids a set of weapons to use against the U.S. Goliath.

The difficulty comes in attempting to define the severity of these threats. Anecdotal evidence on past and present events, while plentiful, is not useful in this regard because it is not clear whether these anecdotes represent the tip of the iceberg or a nearly exhaustive list of all incidents. Better evidence is hard to come by, partly because data are simply difficult to obtain and partly because some classes of victims (e.g., banks and other financial institutions) have every incentive to keep such incidents quiet. That considerably complicates both diagnosing and solving problems related to information vulnerability. It also raises rather complex questions about where the private responsibility of institutions stops and the government's responsibility for protecting the broader public interest starts, as well as where in government the expertise resides to deal with the problem. Even the legal issues associated with the government's gaining detailed enough knowledge about private information systems to protect them adequately and with sharing information on computer vulnerability with private organizations are likely to be formidable.

It is difficult to know the magnitude of the potential problem without examining the vulnerabilities and failure modes of the countless information systems upon which various parts of our national interests depend. The electronic funds transfer network, the air traffic control system, and the electric power grid control system are only a few of the many pieces of the information infrastructure on which our national interests rest. Each of these is protected to some degree from some set of threats; however,

all are in some sense vulnerable (the list of incidents is quite long; e.g., a farmer burying a dead cow accidentally cut a fiber optic cable, closing four of the FAA's 20 air traffic control centers for over five hours in May 1991). Locating and correcting these vulnerabilities should be a national priority if the United States takes the threat of information warfare seriously. The challenge facing a potential adversary is to find the vulnerabilities and exploit them before they are corrected. *It is hard to tell at this point who is likely to win this contest.*

The responsibility for the protection of the National Information Infrastructure has been given (by the Computer Security Act of 1987) to the National Institute of Standards and Technology and to the National Computer Security Center, which is a part of the NSA. Neither of these agencies has the budget, power, or expertise to effect real changes in the manner that computer systems vital to the national interest are protected; most importantly, they do not have any legal right to do so when those systems are owned and operated by private companies, as are the electric power grid, telephone networks, etc. Nor can they alone adjudicate questions of competing military and civilian interests.

NSA involvement is a particularly delicate political and legal issue, given NSA's primary mission as a collector of foreign intelligence and designer of U.S. cryptography systems. However, NSA probably also has the largest concentration of expertise on information security in the U.S. government, so involving it in some politically and legally acceptable maneuver would appear to be essential unless its technical skills and experience could be replicated elsewhere somehow. Otherwise, the task is likely to be left to organizations, such as the Federal Bureau of Investigation, that have appropriate charters but lack the expertise or the organizational culture to do the job effectively. Some sort of interagency approach or even a public-private consortium that enlists the skills of industry experts might eventually prove adequate. If it develops sufficient expertise in the area, the Air Force could be a player, as well as part of an interagency team. That would certainly be a different sort of role for the Air Force, but one that might be both important and appropriate for the future.

None of this is likely to happen, however, until there is a national policy that defines the national interest in the information arena, establishes a mechanism for setting priorities among computing objectives, and assigns responsibility for enforcement. Establishing such a national policy should be a priority item. The need has certainly been recognized.[21] Action is pending to formulate a national strategy on information war.[22]

FINAL OBSERVATIONS

The U.S. military already has a problem. It is shrinking in size and available resources while groping to define an appropriate role in the post–Cold War world. It has already staked much of its future effectiveness on new weapon systems, such as precision-guided weapons and stealthy vehicles, that depend critically on information. Thus, *broad U.S. military strategy could fail if the United States does not deal effectively with information-related issues.*

The problems go far beyond the military. There is a clear need to establish priorities among national goals. However, *there is currently no national policy assigning responsibility for protecting the U.S. civilian sector from "information attacks," defining the national interest in this area, or establishing priorities and resolving conflicts among potentially competing objectives.* Absent such a national policy and a mechanism for implementing it, major problems will remain unsolved, some agencies will knock heads competing for turf and resources, and others will operate at cross purposes. Similarly, the services and the other national security–related agencies need to have an effective process for coordinating their efforts on common problems.

A major part of the problem has been a failure to think and talk properly about the impact of the new information technologies on future warfare and national security. The "information warfare" jargon has gotten in the way. In general, information technology is an "enabling function" that may allow more effective, perhaps new, approaches to warfare and create new classes of potential national security problems as well. However, for the immediate future at least, information is *not* likely to be an appropriate integrating principle, either strategically or organizationally, as the expression "information warfare" implies. Instead, "information warfare" needs to be broken down into its various components, and *those* needed to be integrated effectively into the full range of military operations. That is why policymakers should be focusing on two broader themes: how to protect U.S. security and how to conduct warfare in the information age.

The prime movers in the current Air Force efforts to grapple with information warfare appear to understand the broader issues in spite of the jargon problems. However, that has not prevented confusion elsewhere in the Air Force and risks making the institutionalization of the process overly dependent on personalities. That is obviously a concern if the institutional solution they have created is to be effective beyond their tenures. At best, the process of wrestling with the jargon appears to have been tortuous and tedious and many or may not lead to an effective institutional solution.

Our preliminary analysis suggests that the Air Force's priorities for waging war in the information age should be:

1. Integrating information systems and concerns effectively into "normal" combat operations
2. Designing an information architecture and infrastructure that is robust against casual meddling, enemy action, or "bad karma"
3. Denying enemies the effective use of information using whatever means are most appropriate.

The single most important thing the Air Force has to do in this arena is to integrate information technologies and concerns effectively into the full spectrum of its current operations. That means, among other things, solving all of the problems associated with developing and supporting such advanced weapons as precision-guided munitions, developing a robust and effective information architecture and infrastructure, and establishing suitable career paths for personnel with information-related expertise without unduly isolating them from other parts of the Air Force. As a practical matter, the Air Force needs to disaggregate the various elements that are sometimes lumped together as "information warfare"—e.g., computer security, information-based psychological operations, adaptive planning and battle management, precision strike, attacks with "information weapons"—into more logically coherent pieces that can be integrated more effectively into its operations. This need for better integration of information-related activities into the mainstream of Air Force operations both precedes and transcends the current information-warfare discussion. The process is improving in some areas. Whether it has improved enough remains an issue.

Next, the Air Force needs to protect its information systems against attack or tampering so that its information-based strategy will be effective against competent enemies. Defining the nature and extent of potential threats and choosing the most appropriate, cost-effective ways to protect the full range of information systems on which the Air Force relies requires rigorous analysis of a broad spectrum of options. The Air Force currently appears to be attaching high priority to solving information vulnerability problems, as it should.

Attacking enemies' information systems has always been part of war making, and new technological approaches offer more possibilities for doing that both now and in the future. However, the new kinds of weapons that can attack information systems (e.g., computer viruses, microwave weapons) need to be subjected to the same kind of analytic scrutiny as other weapon systems to see where they fit in the overall scheme of things and under what conditions they offer particular advantages. There is also the broader question of determining against what kind of enemies the whole information-intensive approach to war is likely to work well and how likely the United States is to have to fight such enemies. Dealing with this set of analytical issues should inform both investment decisions and fundamental questions about how to structure the U.S. national security apparatus.

Managing the organizational side of the transition is important as well. The Air Force should proceed with caution in embracing information technology wholesale and perhaps in organizing around information technologies. Although in some areas the Air Force needs to play serious catch-up ball, there is a danger in moving too quickly in others and reorganizing prematurely. In particular, new "information warfare" organizations may miss their niches entirely because of ineffective integration and isolation. On the other hand, established organizations that "talk the talk" might be able to preclude subsequent organizational evolution effectively if they do not develop substantive understanding to accompany the jargon. That is why designing organizational structures that can evolve is so important and why premature restructuring of organizations is so risky. *The Air Force should create an organizational structure and process that will permit integrated analysis of information-related issues and permit an evolution toward a more information-dominated Air Force if and when it is warranted.* So far, the Air Force appears to have avoided some of the worst potential pitfalls, but the battle is not yet over.

Information warfare is clearly the current fad and might or might not prove to be the wave of the future, depending on how events unfold and what rigorous, systematic analysis shows about the relative importance of various elements of information warfare. A real danger is that the faddish aspects could impede the very trends that could make it the wave of the future. As one particularly astute observer put it:

> The history of information technology can be characterized as the overestimation of what can be accomplished immediately and the underestimation of long-term consequences.[23]

NOTES

[1]The burgeoning literature in this field is already vast. The following are some examples. Builder presents a scholarly view of the microchip as a truly revolutionary device (Carl H. Builder, "Is It a Transition or a Revolution?" *Futures*, March 1993, pp. 155–167). The Tofflers have popularized the theme of information-as-the-instrument-of-revolution in warfare and in society in

general for a general audience (Alvin Toffler, *The Third Wave*, New York: Morrow, 1980; Alvin and Heidi Toffler, *War and Anti-war*, Boston: Little, Brown, and Company, 1993). The jargon developed by the Tofflers is in widespread use, even within the national security establishment. Among the military services, the Army, in particular, has adopted the "Third Wave" jargon in describing the importance of information in future warfare. Others have also popularized the idea of "information warfare" (Winn Schwartau, *Information Warfare*, New York: Thunder's Mouth Press, 1994). All of the services have position papers that are currently being updated and revamped. For example, the Air Staff's position on information warfare has evolved (and improved) considerably over the last year or so, as comparisons between early work (e.g., Lt Col David F. Todd, "Exploring Future Concepts of Information Warfare," HQ USAF, Strategic Planning Division, Deputy Chief of Staff for Plans and Operations, January 31, 1994) and current offerings (i.e., Maj Gen Robert Linhard and Maj Gen Kenneth Minihan, "USAF Information Warfare," Briefing, March 3, 1995) clearly indicate. The current Air Force Chief of Staff, Gen Ronald R. Fogelman, has clearly signaled his interest in the effects of information technology on warfare and the importance he attaches to it (Gen Ronald R. Fogelman, *Fundamentals of Information Warfare—An Airman's View*, NSIA-NDU Conference on the Global Information Explosion, May 16, 1995). Furthermore, General Fogelman and Secretary of the Air Force Sheila E. Widnall have jointly endorsed an official Air Force position paper on information warfare (Department of the Air Force, *Cornerstones of Information Warfare*, 1995). In the broader public arena, *Time* magazine has devoted a cover and two articles to "cyberwar" (Douglas Waller, "Onward Cyber Soldiers," *Time*, August 21, 1995, pp. 38–44; Mark Thompson, "If War Comes Home," pp. 44–46, *Time*, August 21, 1995). Certainly the most fun—and perhaps even the most prescient—are the military melodramas, such as Tom Clancy, *Debt of Honor*, New York: Putnam, New York, 1994.

[2]RAND, for example, has ongoing research in all of its national security–related divisions on the impact of information on military operations and overall U.S. national security. In addition, in 1994, RAND created a Center for Information Revolution Analysis to focus research on the effects of the information revolution on society.

[3]Sun Tzu, *The Art of War*, New York: Delacorte Press, 1983, particularly pp. 18, 27–28, 77–82.

[4]The revolution in military affairs, as defined by Andrew Marshall, Director of Net Assessment in the Office of the Secretary of Defense, is currently viewed as having three major elements: information warfare, precision strike, and dominant maneuver. (There is some speculation that space could be added as a fourth element, although it seems redundant with some aspects of the original three.) The working hypothesis is that the confluence of these elements could result in revolutionary changes in the art of war. (For a more detailed discussion, see Jeffrey McKitrick et al., "The Revolution in Military Affairs," Science Applications International Corporation, December 1994.) For some of the reservations about the "revolution in military affairs," as well as its potential advantages, see John T. Cornell, "Signs of a Revolution," *Air Force Magazine*, August 1995, p. 2, and John Barry, "The Battle Over Warfare," *Newsweek*, December 5, 1994, pp. 27–28.

[5]We are certainly not the first to notice, or be annoyed by, "cyberbabble." The critics range from the serious (John A. Barry, *Technobabble*, Cambridge, Mass.: MIT Press, 1992) to the whimsical (Russell Baker, "A Little Cyber Grouch," *New York Times*, March 25, 1995, p. 15).

[6]The current Air Force definition of *information warfare* is: "Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own information operations." (AFDC1W 2000 Draft, March 7, 1995, p. 3). This is by no means universally accepted. Others tend to emphasize electronic attack and defense and exclude the broader notion of "information operations" from the definition of information warfare. Still others forgo the expression of information warfare entirely and use more-precise language.

[7]For the views of another author who finds the term "information warfare" most unfortunate, see Martin C. Libicki, "What is Information Warfare?" *Strategic Forum*, Institute for National Strategic Studies, National Defense University, May 1995.

[8]Libicki (1995). Libicki makes the same point in defining seven classes of information-related operations, each of which needs to be appreciated on its own merits rather than lumped together under the single rubric of "information warfare."

[9]For a brief, unclassified summary of the B-2 analysis, see Glenn C. Buchan and David R. Frelinger, *Providing an Effective Bomber Force for the Future: The B-2 Debate in Perspective*, Santa Monica, Calif.: RAND, CT-134, May 1995.

[10]For detailed discussions of some of the problems and potential solutions, see Myron Hura and Gary McLeod, *Route Planning Issues for Low Observable Aircraft and Cruise Missiles: Implications for the Intelligence Community*, Santa Monica, Calif.: RAND, MR-187-AF, 1993a; Myron Hura and Gary McLeod, *Intelligence Support and Mission Planning for Autonomous Precision-Guided Weapons: Implications for Intelligence Support Plan Development*, Santa Monica, Calif.: RAND, MR-230-AF,

1993b; Myron Hura and Gary McLeod, *Producing Target Models at a Central Facility: Assessment Methodology*, Santa Monica, Calif.: RAND, MR-425-AF, 1994; and Myron Hura and Gary McLeod, *Ensuring Adequate Intelligence Support for the Acquisition of New Weapon Systems*, Santa Monica, Calif.: RAND, DB-125-CMS, 1995.

[11]ISPs are described in Department of the Air Force, *Acquisition Management Policies and Procedures*, AF Supplement 1 to DoD Instruction 5000.2, August 31, 1993 (see Part 7, Section C, "Infrastructure Support"); Department of the Air Force, Intelligence Support to the Air Force Acquisition Process, AF Instruction 14-208, March 21, 1994a; and Department of the Air Force, *Air Force Mission Needs and Operational Requirements: Guidance and Procedures*, AF Instruction 10-601, May 31, 1994b.

[12]For discussions of some of the problems of career intelligence officers, see forthcoming works by former RAND Air Force Fellows Majors Larry Hollett and Ed O'Connell.

[13]Meetings with the Air Force C^4 Agency; AFDC/W2000 Draft (1995).

[14]Quoted from Internet: "DISA Stings Uncover Computer Security Flaws," *Federal Computer Week*, February 6, 1995.

[15]R. O. Hundley and R. H. Anderson, Security in *Cyberspace: An Emerging Challenge for Society*, Santa Monica, Calif.: RAND, P-7893, December 1994.

[16]AF/SC, *Road Map for Info Protect*, 1995.

[17]For examples of this type of offensive "information warfare," see John Arquilla and David Ronfeldt, *Cyberwar Is Coming!* Santa Monica, Calif.: RAND, P-7791, 1992.

[18]Manuel deLanda, *War in the Age of Intelligent Machines*, Cambridge, Mass.: MIT Press, 1991.

[19]The creation of the Information Warfare Squadron at 9th Air Force Headquarters illustrates both the organizational problems and the complications that jargon can cause. On the one hand, creating such a group at an operational command may help focus attention at the operations level, where it belongs. On the other hand, what is the squadron to do? Obviously, it cannot handle the breadth of information warfare, which the Air Force defines as including information operations, defense of Air Force information systems, and attack of enemy information systems. Information operations alone include a large part of what an operational Air Force does. The squadron could focus on protecting Air Force information systems, but there is already a large organization (SC–command, control, and communications) at 9th Air Force that has more manpower and expertise and should logically have that charter. It might be able to find a niche in offensive information operations, an area that is probably less well-represented currently in the 9th Air Force structure. However, such an offensive information-warfare cell should really be integrated with the offensive planners who employ more traditional weapons to attack a full spectrum of enemy targets, including those associated with information. Thus, why an Information Warfare Squadron? Ironically, it might eventually prove a useful vehicle for focusing the attention of the rest of the Air Force on the needs of the operators for information-related support and providing a suitable organizational nexus. However, this is a relatively Byzantine way to solve the institutional problems, and it could backfire in several different ways. It will be interesting to see how it evolves.

[20]Cornell (1994), makes this point as well.

[21]To aid in formulating a national policy in this area, the Director of Central Intelligence has directed the National Intelligence Officer for Science and Technology to produce a National Intelligence Estimate on information warfare by mid-1996.

[22]Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," *Washington Post*, July 16, 1995, p. C3.

[23]Paul Strassman, *Information Payoff: The Transformation of Work in the Electronic Age*, New York: Free Press, 1985, p. 199. We want to thank our colleague David Ronfeldt for bringing this work to our attention.

RAND
1700 Main Street, P.O. Box 2138, Santa Monica, California 90407-2138 • Telephone 310-393-0411 • FAX 310-393-4818
2100 M St., N.W., Washington, D.C. 20037-1270 • Telephone 202-296-5000 • FAX 202-296-7960

IP-149